IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



| | |
|---|---|
| In re appl. of: **Benantar** | § Group Art Unit: **2131** |
| Serial No.: **09/734,809** | § Examiner: **Vaughan, M.** |
| Filing Date: **12/11/2000** | § Atty. Docket #: **AUS9-2000-0799-US1** |
| For: **Method and system for a secure binding of a revoked X.509 certificate to its corresponding certificate revocation list** | § |

**Certificate of Mailing**
**Under 37 C.F.R. § 1.8(a)**

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to:
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450
on October 18, 2004.

By: [signature]
Joseph R. Burwell, Reg. No 44,468

**RESPONSE TO OFFICE ACTION UNDER 37 C.F.R. § 1.111**

The following remarks are offered in response to the Office Action mailed 06/17/2004; a petition for an extension of time is included with this response.

No additional fees are believed to be necessary for this response; if, however, any fees are necessary, please charge Deposit Account No. 50-1888 of Joseph Burwell to cover the cost of the fees.

## I. General Remarks Concerning This Response

Claims 1-32 are currently pending in the present application. No claims have been amended, added, or canceled in this response. Reconsideration of the claims is respectfully requested.

The Office action has acknowledged the receipt of informal drawings that were filed with the application. However, a set of formal drawings were filed with the PTO on 05/25/2001. Applicant requests an acknowledgment of the receipt of those formal drawings in the next PTO communication along with an indication of whether or not the formal drawings are acceptable.

## II. Summary of Present Invention

A method, system, apparatus, and computer program product are presented for enabling an application that is validating a certificate to have a high level of assurance when checking the membership of a certificate within a particular certificate revocation list. First, the application checks whether a certificate's serial number is found within a certificate revocation list, and if there is a successful comparison within the serial numbers, then the fingerprint of the certificate is computed, preferably based on the digest algorithm specified by the certificate revocation list. The computed fingerprint is then compared to the certificate's fingerprint as previously stored within the certificate revocation list. If there is a successful comparison between the fingerprints, then the certificate can be properly invalidate or rejected, thereby lessening the chances that a valid certificate would be improperly rejected or invalidated.

**III. <u>35 U.S.C. § 103(a)–Obviousness–*Van Oorschot* in view of *RFC 2459*</u>**

The Office action has rejected claims 1-32 under 35 U.S.C. § 103(a) as unpatentable over Van Oorschot et al., "Method for Efficient Management of Certificate Revocation Lists and Update Information", U.S. Patent 5,699,431, filed 11/13/1995, issued 12/16/1997, in view of IETF's RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999. This rejection is traversed.

With respect to the first through the fourth elements of independent claims 1, 11, and 21, the rejection begins by stating the following :

> As per claims 1, 11, and 21, Van Oorschot teaches a method for validating a digital certificate within a data processing system, the method comprising: receiving a digital certificate (col. 1, line 50); retrieving a certificate revocation list (col. 1, line 61-62); extracting a first serial number from the digital certificate, wherein the first serial number has been associated with the digital certificate by a certifying authority (col. 2, lines 7-8); determining whether the first serial number matches a second serial number stored within the certificate revocation list (col. 2, line 8). Van Oorschot teaches that a match in the serial number means that the certificate has been revoked. Van Oorschot teaches that in the certificate is option information that specifies where additional access information as disclosed by Van Oorschot is the particular CA that was used to certify that particular certificate (col. 5, lines 13-24). Van Oorschot's system can be applied to the X.509 standard of digital certificates. Here is the format of a X.509 certificate: ...

Applicant does not dispute these statements in the rejection; these elements recite well-known processing steps for checking whether a digital certificate has been revoked as indicated within a certificate revocation list.

However, the claims are directed to a novel method, apparatus, etc., for determining whether a digital certificate has been revoked by performing additional steps or including

means for performing additional processing. The fifth and sixth elements of claim 1 recite the following:

> in response to a determination that the first serial number matches the second serial number, computing a first certificate fingerprint for the digital certificate; and
>
> comparing the first certificate fingerprint with a second certificate fingerprint stored within the certificate revocation list, wherein the second certificate fingerprint is associated with the second serial number.

Applicant asserts that the applied prior art references do not disclose these elements, notwithstanding the statements in the rejection to the contrary.

The rejection addresses claims 1, 11, and 21 together as a corresponding method, an apparatus, and a computer program product, and Applicant hereinbelow uses claim 1 as an exemplary claim. In addition, independent claims 7, 17, and 27 are similar to each other; these claims reflect the creation of a novel CRL that includes certificate fingerprints. Also, independent claim 31 is directed to a special CRL data structure. The Office action has used similar logic in rejection claims 7, 17, 27, and 31 along with claims 1, 11, and 21, and Applicant relies on the arguments that are presented with respect to claim 1 to address claims 7, 17, 27, and 31.

With respect to the fifth element of claim 1, the rejection states: "Van Oorschot teaches computing a first certificate fingerprint for the digital certificate (col. 5, lines 39-40)." The portion of <u>Van Oorschot et al.</u> that is referenced at column 5, lines 39-40 states the following: "In a further embodiment, the address_list field value embedded in a certificate is the one-way hash of a (typically longer) address_list value; this allows some savings in storage." As noted earlier in the rejection, <u>Van Oorschot et al.</u> discloses the inclusion of additional access information that is used to certify a particular certificate; more specifically, as stated at column 5, lines 21-24:

> The address_list field is a list of values identifying, explicitly or implicitly, one or more distribution points at which a CRL associated with the certificate in question may be found. An application using the certificate may obtain from this location a CRL, to ascertain if the certificate in question has been revoked.

Using this information, Applicant disagrees that Van Oorschot et al. discloses the fifth element of claim 1 for the following reasons, all of which are interrelated.

First, while Van Oorschot et al. discloses that a portion of the information in a certificate may be a hash value, it specifically states that the hash value is used in order to save storage space. Although this hash value is not described further, one can surmise from the preceding statements that the hash value is probably used as a lookup value within a hash table to determine a longer form of the address_list value; after looking up the needed information within a hash table to obtain a full address_list value, a system would then use the address information to find the certificate information or certificate revocation list information to process or validate the certificate. Therefore, although Van Oorschot et al. discloses the generation of a hash value, the hash value is not used as a digital fingerprint.

Second, for a hash value to be considered as a digital fingerprint, one needs the original information to be present in order to generate the hash value that represents a digital fingerprint of the information; one can then use the digital fingerprint to verify or to validate the original information. In other words, a digital fingerprint is generated by using information, such as a digital certificate, as input into a hashing algorithm in order to check the validity of that original information. In Van Oorschot et al., the hash value may be "embedded in a certificate"; since the original address_list value is not embedded in the certificate, the hash value cannot be used to validate the original address_list information.

Therefore, the hash value that is referenced by the rejection is not equivalent to the digital fingerprint of the present invention; although the data formats may be similar as outputted by a hashing algorithm, they are used for different purposes to achieve different results.

Third, the hash value in Van Oorschot et al. is generated by the certificate authority that creates the digital certificate in which the hash value is included. In the present invention, the digital fingerprint is generated by the entity that is determining the validity of a digital certificate. This further supports Applicant's assertion that the hash value in Van Oorschot et al. and the digital fingerprint of the present invention are not equivalent.

Fourth, the hash value in Van Oorschot et al. is generated by using only the original address_list value as input, i.e. a single data item. In contrast, the present invention generates the digital fingerprint by using the entire digital certificate ("Certificate fingerprint 422 is computed using a particular digest algorithm over the revoked certificate."--page 18, lines 29-30). Moreover, the term "certificate fingerprint" in the claim language was used to relate that a digital fingerprint is computed over an entire digital certificate. Again, this supports Applicant's contention that the hash value in Van Oorschot et al. and the digital fingerprint of the present invention are not equivalent.

Fifth, the claim element states that the processing step that is recited by the fifth element of claim 1 is performed "in response to a determination that the first serial number matches the second serial number"; in other words, this step is one of the additional novel steps that are used in determining whether the digital certificate has been revoked. Van Oorschot et al. does not perform these steps, and more specifically, Van Oorschot et al. does not perform the step in the fifth element "in

response to a determination that the first serial number matches the second serial number".

Turning to the remainder of claim 1, the sixth element of claim 1 recites the following:

> comparing the first certificate fingerprint with a second certificate fingerprint stored within the certificate revocation list, wherein the second certificate fingerprint is associated with the second serial number.

With respect to the sixth element of claim 1, the rejection states:

> Van Oorschot does not explicitly teach comparing the first certificate fingerprint with a second certificate fingerprint stored within the certificate revocation list, wherein the second certificate fingerprint is associated with the second serial number.

The rejection then turns to RFC 2459 for support, and the rejection continues:

> From the format of the X.509 certificate one of ordinary skill in the art would know that the additional information included in the certificate of Van Oorschot to identify a particular CA is essentially an issuer unique identifier. As stated by RFC 2459, this optional field is used to avoid ambiguousness of CA over time. In fact both the issuer and subject unique identifiers are designed to avoid conflicts of possible reuse of an issuer or subject name. Therefore both fields represent fingerprinting data because they provide uniqueness. Van Oorschot teaches that this value can be embedded in a certificate (col. 5, lines 39-40) and that it should be verified (col. 2, lines 59-61). It would then be advantageous to match this optional information, which the additional information stored at the CRL [sic], similarly to how the serial numbers are matched. Further evidence of matching is suggested by Van Oorschot teaches [sic] that the additional information is also kept at a second location (one other than on the certificate itself) (col. 4, lines 5-7). To summarize, based on the optional fields of the x.509 standard, it would have been obvious to use the additional access information taught by Van Oorschot as a further matching/verification parameter to determine if a certificate is revoked.

Applicant asserts that this argument is problematic for multiple reasons.

First, the rejection stated with respect to the fifth element that the step of "computing a first certificate fingerprint for the digital certificate" is equivalent to the hash value of the address_list value in the system of Van Oorschot et al.. However, the sixth element references the same "first certificate fingerprint", yet when the rejection addresses the sixth element with respect to Van Oorschot et al., the rejection does not mention of the use or the comparison of anything to the hash value of the address_list value in the system of Van Oorschot et al.. In other words, the logical foundation of the rejection's argument that was started with respect to the fifth element is completely ignored with respect to the sixth element; the logic does not follow. The rejection had started an argument that a certificate fingerprint is equivalent to the hash value for the address_list value, but then the rejection begins to argue that other data fields act as "fingerprinting data". Moreover, there would be no reason for comparing the hash value for the address_list value to some other value as required by the comparison step in the sixth element of claim 1.

Second, the specification is clear is its description of a "certificate fingerprint" as being generated by inputting a digital certificate into a digest algorithm or a hashing algorithm in order to generate a digital fingerprint over the digital certificate; the terminology in the claim language follows the description in the specification of the present patent application. Moreover, Applicant's use of the terminology is consistent with the ordinary meaning of a "digital fingerprint" as applied in a specific instance to a digital certificate. For example, the following quote is taken from the following web address: www.itep.ae/english/EducationCenter/InternetConcepts/m_digest.asp

What is a message digest?

When a message is encrypted using the RSA system, it can also request a hash function. A hash function is the mathematical computation applied to a message in order to generate a digest (small string) that will represent the whole file or message (large strings). This resulting data is called the message digest.

**A message digest serves as the digital fingerprint of a message.** It is of fixed-length (usually 128 to 160-bits) whatever the length of the original message is. Viewing the message digest alone will not reveal the contents of the original message. Changing even a single bit on the message will result in a totally different output value.

It is also impossible to come up with an identical message digest derived from two different messages. Every message digest created by a private key is unique to the creator, and can only be decrypted using the corresponding public key. Hence, a message digest is also known as a "one-way hash function".

In contrast, the rejection must present a complex argument as to how certain data could be used to "provide uniqueness" in a manner that is supposedly equivalent to the manner in which the present invention has used a digital fingerprint. It should be apparent to one having ordinary skill in the art that the rejection's argument is convoluted because neither Van Oorschot et al. nor RFC 2459 disclose the use of digital fingerprints over digital certificates in conjunction with CRLs in a manner that is equivalent to the processing that is used by the present invention.

Applicant also asserts that the motivational statement in the rejection has obtained the motivation for combining the applied prior art references from Applicant's own disclosure. The motivational statement states:

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of RFC 2459 within the system of Van Oorschot because it would prevent ambiguousness of certificates in the event that names were reused by the certificate authority.

This is borrowed from the specification of the present patent application. For example, on page 22, the present application states:

> ... it is highly unlikely that the certifying authority would issue two certificates with identical serial numbers to two different entities with the same subject name, key usage, and extensions. Hence, the certificate fingerprints would be different even if the serial numbers were the same.

The prior art does not disclose a concern about improperly identifying a digital certificate within a certificate revocation list. The portions of RFC 2459 to which the rejection points illustrates a concern only for the inadvertent creation of two identical digital certificates. Thus, the rejection has used an improper amount of hindsight in applying Applicant's own disclosure against Applicant's own claims.

Dependent claims 2-6, 8-10, 12-16, 18-20, 22-26, 28-30, and 32 recite further limitations that are not present within the independent claims from which they depend. For example, the dependent claims recite X.509 formatting, etc.. However, since the dependent claims incorporate the features of the independent claims, the rejections of the dependent claims are similarly deficient for the same reasons that were argued above with respect to the independent claims.

More specifically, dependent claims 6, 10, 16, 20, 26, and 30 recite the computation of a certificate fingerprint using a digest algorithm identifier that is stored with the second certificate fingerprint, i.e. within a CRL. In other words, one must interpret the certificate fingerprint within the independent claims as being generated through the use of a digest algorithm. When these dependent claims are interpreted together with the limitations from the independent claims, the rejection's argument about using certain data items as "representing fingerprinting data because they provide uniqueness" is especially illogical.

Examiner bears the burden of establishing a *prima facie* case of obviousness

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Only when a *prima facie* case of obviousness is established does the burden shift to the applicant to produce evidence of nonobviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Rijckaert*, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). If the Patent Office does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). In response to an assertion of obviousness by the Patent Office, the applicant may attack the Patent Office's *prima facie* determination as improperly made out, present objective evidence tending to support a conclusion of nonobviousness, or both. *In re Fritch*, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780, 1783 (Fed. Cir. 1992).

Van Oorschot et al. and RFC 2459 clearly fail to disclose at least one feature of the present invention as recited within each independent claim, notwithstanding the arguments presented by the Office action, thereby rendering Van Oorschot et al. and RFC 2459 incapable of being used as primary and secondary references as argued by the current rejection. Moreover, a hypothetical combination of Van Oorschot et al. and RFC 2459 would also fail to reach the claimed invention of the present patent application. As should be recognized, because both the primary and secondary references in the rejection fail to disclose the claimed features against which the references were applied, and because the references fail to be combinable to produce these claimed

features, the rejection fails to fulfill the requirements of a proper obviousness argument.

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

**IV. Conclusion**

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: October 18, 2004

Respectfully submitted,

Joseph R. Burwell
Reg. No. 44,468
ATTORNEY FOR APPLICANT

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755-8022
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz